Received: 10/30/2003

2003 DRAFTING REQUEST

Assembly Substitute Amendment (ASA-AB584)

Received: 10/30/2003 Wanted: Soon For: Marlin Schneider (608) 266-0215					Received By: rnelson2 Identical to LRB: By/Representing: Cynthia												
									This file	may be shown	to any legislat	or: NO		Drafter: rnelson2 Addl. Drafters: Extra Copies:			
									May Co	ntact:							
Subject:	Courts	- evidence															
Submit	via email: YES																
Request	er's email:	Rep.Schne	ider@legis.	state.wi.us													
Carbon	copy (CC:) to:				* .												
Pre Top	pic:	· · · · · · · · · · · · · · · · · · ·	***************************************			-											
No spec	ific pre topic gi	ven		•													
Topic:	The Management of the Manageme																
Use of d	ligital technolog	gy in evidence	only if canno	ot be altered													
Instruc	tions:	·															
See Atta	iched						* · · · · · · · · · · · · · · · · · · ·										
Draftin	g History:					······································											
Vers.	Drafted	Reviewed	Typed	Proofed	Submitted	<u>Jacketed</u>	Required										
/? /P1	rnelson2 10/30/2003	jdyer 11/03/2003 jdyer 11/04/2003	jfrantze 11/04/200	03	lemery 11/04/2003												
/1	rnelson2	jdyer	jfrantze		lnorthro	lnorthro											

11/04/2003 12:21:32 PM Page 2

Vers.	<u>Drafted</u>	Reviewed	Typed	Proofed	Submitted	<u>Jacketed</u>	Required
	11/04/2003	11/04/2003	11/04/2003	3	11/04/2003	11/04/2003	

FE Sent For:

<**END**>

2003 DRAFTING REQUEST

Assembly Substitute Amendment (ASA-AB584)

Received: 10/30/2003 Wanted: Soon For: Marlin Schneider (608) 266-0215					Received By: rnelson2				
					Identical to LRB: By/Representing: Cynthia				
This file	may be shown	to any legislato	or: NO		Drafter: rnelson	12			
May Co	ntact:				Addl. Drafters: Extra Copies:				
Subject:	Courts	- evidence							
Submit v	via email: YES	•							
Requesto	er's email:	Rep.Schne	ider@legis.	state.wi.us					
Carbon o	copy (CC:) to:								
Pre Top	oic:						·		
No speci	ific pre topic gi	iven							
Topic:									
Use of d	igital technolog	gy in evidence o	only if canno	ot be altered					
Instruct	tions:	<u> </u>							
See Atta	ched								
Draftin	g History:								
Vers.	Drafted	Reviewed	Typed	Proofed	Submitted	Jacketed	Required		
/? /P1	rnelson2 10/30/2003	jdyer 11/03/2003 jdyer 11/04/2003	jfrantze 11/04/200	03	lemery 11/04/2003				
		1 1/4 ; id	do 11/4	Jelf 11/4					

11/04/2003 09:25:04 AM Page 2

FE Sent For:

<END>

2003 DRAFTING REQUEST

Assembly Substitute Amendment (ASA-AB584)

Received: 10/30/2003 Received By: rnelson2

Wanted: Soon Identical to LRB:

For: Marlin Schneider (608) 266-0215 By/Representing: Cynthia

This file may be shown to any legislator: **NO**Drafter: **rnelson2**

May Contact: Addl. Drafters:

Subject: Courts - evidence Extra Copies:

Submit via email: YES

Requester's email: Rep.Schneider@legis.state.wi.us

Carbon copy (CC:) to:

Pre Topic:

No specific pre topic given

Topic:

Use of digital technology in evidence only if cannot be altered

Instructions:

See Attached

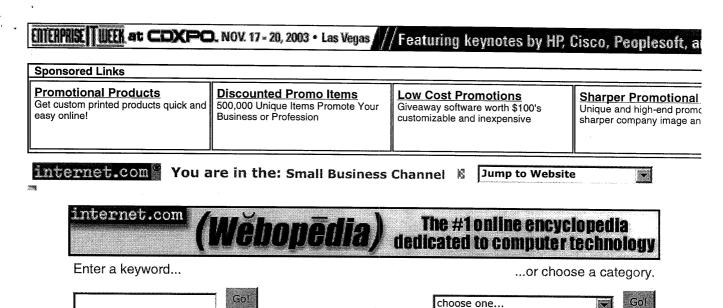
Drafting History:

<u>Vers.</u> <u>Drafted</u> <u>Reviewed</u> <u>Typed</u> <u>Proofed</u> <u>Submitted</u> <u>Jacketed</u> Required

/? rnelson2 /PI // A / PA

FE Sent For:

<END>



MENU

Home
Term of the Day
New Terms
New Links
Quick Reference
Did You Know?
Search Tool
Tech Support
Webopedia Jobs
About Us
Link to Us
Advertising

Compare Prices:



Submit a URL
Suggest a Term
Report an Error



Developer DevX Downloads

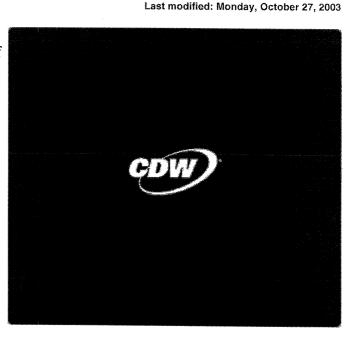
digital watermark

Also referred to as simply watermarking, a pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information (author, rights, etc.). The name comes from the faintly visible watermarks imprinted on stationery that identify the manufacturer of the stationery. The purpose of digital watermarks is to provide copyright

protection for intellectual

property that's in digital

format.



Unlike printed watermarks, which are intended to be somewhat visible, digital watermarks are designed to be completely invisible, or in the case of audio clips, inaudible. Moreover, the actual bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated. And finally, the digital watermark must be robust enough so that it can withstand normal changes to the file, such as reductions from <u>lossy</u> compression algorithms.

Satisfying all these requirements is no easy feat, but there are a number of companies offering competing technologies. All of them work by making the watermark appear as <u>noise</u> - that is, random data that exists in most digital files

EarthWeb
Graphics
Interactive Marketing
International
Internet Lists
Internet News
Internet Resources
IT
Linux/Open Source
Small Business
Windows Technology
Wireless Internet
xSP Resources

Search internet.com
Advertise
Corporate Info
Newsletters
Tech Jobs
E-mail Offers

internet commerce

Be a Commerce Partner
Submit Your Site
Register Domains
Reference Library
Revenue Share With Us
Best Deals on PDAs!
Find a Consultant
Shop Digital Cameras
Web Hosting
Search Web Hosting
Business Search

anyway. To view a watermark, you need a special program that knows how to extract the watermark data.

Watermarking is also called data embedding and information hiding.

•E-mail this definition to a colleague•

Sponsored Listings

For internet.com pages about **digital watermark CLICK HERE**. Also check out the following links!

LINKS

∋!'€ = Great Page!

DRM Watch 🤾

Analysis of digital rights management technology.

Digital Watermarking Links

Good collection of links to papers on digital watermarking. Also includes a link to the watermarking Webring.

Information Hiding Home Page

Provides a brief history of steganography, with links to image watermarking methods, annotated bibliographies, possible problems and failures, companies, products, research groups and news items.

Look, it's not there

Byte article (January, 1997) by Jian Zhao that describes how digital watermarking works.

Watermarking and Data Hiding Resources

Huge collection of references on multimedia watermarking and data hiding research and technology.

Webreference's Digital Watermark page

Contains links to companies developing digital watermark products, and articles about digital watermarks.

Sponsored Listings

Related Categories

<u>Digital Rights Management</u> (DRM)

<u>Multimedia</u>

Related Terms

copy protection

FlashPix

Product Activation

software piracy

(Wěhonědia)

Give Us Your Feedback

Shopping DIGITAL WATERMARK Products

Compare Products, Prices and Stores

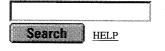
Shop by Category: Graphics and Publishing Software 2 Model Matches

Education and Reference Software

1 Model Matches

Watermarking World





WATERMARKING

- Biography
- FAQ

MAILINGLIST

- Management
- Archive

CONFERENCES

• Calls

BENCHMARKING

- Stirmark
- CheckMark
- Optimark

BOOKS

LINKS

- Companies
- Research
- Others

WEBRING

DISCLAIMER

Digital Watermarking Frequently Asked Questions (FAQ)

Please help us: The FAQs below are preliminary and not complete. Anybody having an answer to an open item is encouraged to <u>send</u> us his contribution. We will continaully work on the FAQs and update them. Thanks!

Last modified: OCT 14, 2001

Introduction

This document tries to answer question frequently asked on the Watermarking mailing list. To join this list, please refer to the subscription information on http://www.watermarkingworld.org/ml.html.

Many people have contributed to this FAQ. In alphabetical order:

- Fabien Petitcolas
- Jong-Hyeon Lee
- Matthieu Brunet
- Stefan Katzenbeisser
- Martin Kutter

General questions

 What is the difference between "copy protection" and "copyright protection"?

Copy protection attempts to find ways, which limit the access to copyrighted material and/or inhibit the copy process itself. Examples of copy protection include encrypted digital TV broadcast, access controls to copyrighted software through the use of license servers and technical copy protection mechanisms on the media. A recent example is the copy protection mechanism on DVDs. However, copy protection is very difficult to achieve in open systems, as recent incidents (like the DVD hack) show. Copyright protection inserts copyright information into the digital object without a loss of quality. Whenever the

copyright of a digital object is in question, this information is extracted to identify the rightful owner. It is also possible to encode the identity of the original buyer together with the identity of the copyright holder, which allows tracing of any unauthorized copies. The most prominent way of embedding information in multimedia data is the use of digital watermarking.

Whereas copy protection seems to be difficult to implement, copyright protection protocols based on watermarking and strong cryptography are likely to be feasible.

What is the difference between visible and invisible watermarking?

Send answer.

What is the watermark?

Although different authors use different meaning for the word 'watermark', it is mostly agreed that the watermark is what is actually imperceptibly added to the cover-signal in order to convey the hidden data.

• Usefulness? Send answer.

What is the original image?

Consider the following scenario: Alice, the copyright holder, inserts her own watermark into some object, locks the original away and keeps selling the marked image. Bob can now try to insert his own watermark into the already marked object. In case of a dispute, both Alice and Bob are able to prove the presence of "their" watermark and claim ownership of the document. How can this situation be resolved?

The "traditional" answer is: look at the objects Alice and Bob claim to be the original. Alice's original should not contain a watermark, whereas Bob's "original" must contain Alice's watermark (if we assume that Bob cannot remove marks). This situation would indicate that Bob inserted his watermark after Alice and so one may conclude that Alice is the rightful owner.

Unfortunately, sometimes the situation is not that simple. It has been shown that a particular class of watermarking schemes, Bob can insert his watermark in a way that it also seems to be present in the copy Alice locked away (although he has no access to it). So Alice's original contains Bob's mark and Bob's "original" contains Alice's mark. This type of attack is called "inversion attack" or more "dead lock attack". There is no way to resolve copyright ownership in this case. This result indicates that watermarking "alone", that is without a carefully designed protocol around it, will not suffice to resolve the copyright situation.

Why not add the copyright information into the file

format?

One could define a new audio file format, in which the watermark is a part of the header block but is not removable without destroying the original signal, because part of the definition of the file format requires the watermark to be therein. In this case the signal would not really be literally 'destroyed' but any application using this file format would not touch it without a valid watermark. Some electronic copyright management system propose mechanisms like this. Such schemes are weak as anyone with a computer or a digital editing workstation would be able to convert the information to another format and remove the watermark at the same time. Finally this new audio format would be incompatible with the existing one. Thus the watermark should really be embedded in the audio signal. This is very similar to S.C.M.S. When Philips and Sony introduced the 'S/PDIF' (Sony/Phillips Digital Interchange Format), they included the S.C.M.S. (Serial Code Management System) which provides a way copies of digital music are regulated in the consumer market. This information is added to the stream of data that contains the music when one makes a digital copy (a 'clone'). This is in fact just a bit saying: digital copy prohibited or permitted. Some professional equipment are exempt for needing S.C.M.S.

With watermarking however, the copy control information is part of the audio-visual signal and aim at surviving file format conversion and other transformations.

What is the difference between watermarking.

steganography, and cryptography?

While cryptography is about protecting the content of messages (their meaning), steganography is about concealing their very existence. It comes from Greek roots, literally means 'covered writing', and is usually interpreted to mean hiding information in other information. Examples include sending a message to a spy by marking certain letters in a newspaper using invisible ink, and adding subperceptible echo at certain places in an audio recording. It is often thought that communications may be secured by encrypting the traffic, but this has rarely been adequate in practice. Æneas the Tactician, and other classical writers, concentrated on methods for hiding messages rather than

for enciphering them; and although modern cryptographic techniques started to develop during the Renaissance, we find in 1641 that <u>John Wilkins</u> still preferred hiding over

preference persists in many operational contexts to this day.

ciphering because it arouses less suspicion. This

For example, an encrypted email message between a known drug dealer and somebody not yet under suspicion.

or between an employee of a defense contractor and the embassy of a hostile power, has obvious implications.

As the purpose of steganography is having a covert communication between two parties whose existence is unknown to a possible attacker, a successful attack consists in detecting the existence of this communication (e.g., using statistical analysis of images with and without hidden information). Watermarking, as opposed to steganography, has the (additional) requirement of robustness against possible attacks. In this context, the term 'robustness' is still not very clear; it mainly depends on the application. Copyright marks do not always need to be hidden, as some systems use visible digital watermarks, but most of the literature has focused on imperceptible (e.g., invisible, inaudible) digital watermarks which have wider applications. Visible digital watermarks are strongly linked to the original paper watermarks which appeared at the end of the XIII century to differentiate paper makers of that time. Modern visible watermarks may be visual patterns (e.g., a company logo or copyright sign) overlaid on digital images. The intent of use is also different: the payload of a watermark can be perceived as an attribute of the cover-signal (e.g., copyright information, license, ownership, etc.). In most cases the information hidden using steganographic techniques is not related at all to the cover. These differences in goal lead to very different hiding techniques.

What are 'public watermarking', 'blind watermarking', 'semi-blind watermarking', 'private watermarking', 'nonblind watermarking' and 'asymmetric watermarking'? There as been some confusion about the naming of various types of watermarking techniques and the main reason is that people involved in this field come from different backgrounds (in particular signal processing and computer security). On top of this some terminology has been imported from the related field of steganography. Originally, public watermarking and blind watermarking mean the same, but the wording was confusing with publickey watermarking and 'signal processing people' took over the field so only the later tends to remain. In these schemes the cover signal (the original signal) is not needed during the detection process to detect the mark. Solely the key, which is typically used to generate some random sequence used during the embedding process, is required. These types of schemes can be used easily in mass market electronic equipment or software.

In some cases you may need extra information to help your detector (in particular to synchronise its random sequence on the possibly distorted test signal). In particular some

watermarking schemes require access to the 'published' watermarked signal, that is the original signal just after adding the watermark. People refer to these schemes as semi-blind watermarking schemes.

Private watermarking and non-blind-watermarking mean the same: the original cover signal is required during the detection process.

At last, by asymmetric watermarking or public-key watermarking, people refer to watermarking schemes with properties reminding asymmetric cryptosystem (or public key cryptosystem). No such system really exists yet although some possible suggestions have been made. In this case, the detection process (and in particular the detection key) is fully known to anyone as opposed to blind watermarking where a secret key is required. So here, only a 'public key' is needed for verification and a 'private key' (secret) is used for the embedding though. Knowledge of the public key does not help to compute the private key (at least in a reasonable time), it does not either allow removal of the mark nor it allows an attacker to forge a mark.

What is the difference between (semi-)fragile and robust watermarks?

The aims of such watermarks are completely different: A (semi-)fragile watermark is a mark which is (highly) sensitive to a modification of the stego-medium. A fragile watermarking scheme should be able to detect any change in the signal and identify where it has taken place and possibly what the signal was before modification. It serves at proving the authenticity of a document. On the opposite, a robust watermark should be stuck to the document it has been embedded in, in such a way that any signal transform of reasonable strength cannot remove the watermark. Hence a pirate willing to remove the watermark will not succeed unless they debase the document too much to be of commercial interest.

The latter form is the very challenging and attracts most research.

What are fingerprints?

Fingerprints are characteristics of an object that tend to distinguish it from other similar objects. They enable the owner to trace authorized users distributing them illegally. In the case of encrypted satellite television broadcasting, for instance, users could be issued a set of keys to decrypt the video streams and the television station could insert fingerprint bits into each packet of the traffic to detect unauthorized uses. If a group of users give their subset of keys to unauthorized people (so that they can also decrypt the traffic) at least one of the key donors can be traced

when the unauthorized decoder is captured. In this respect, fingerprinting is usually discussed in the context of the *traitor tracing* problem.

 What is the oldest (historical) method developed/used for the purpose of ownership protection? The original paper watermarks appeared at the end of the 13thI century to differentiate paper makers of that time. Modern visible watermarks may be visual patterns (e.g., a company logo or copyright sign) overlaid on digital images and are widely used by many photographers who do not trust invisible watermarking techniques enough. In the 17th century, Claude Gellée of Lorraine (1600–1682), also known as Claude Lorrain, introduced a method for protecting his intellectual property nearly hundred years before any relevant law was introduced (the first 'copyright' law was the 'Statute of Anne' introduced by the English Parliament in 1710.) From some time around 1635 until the end of his life in 1682, Lorrain kept a book that he called the Liber Veritatis (now kept in the British Museum in London). The Liber Veritatis was a collection of drawings in the form of a sketchbook. The book was specially made for him, with a scheme of alternating pages, four blue pages followed by four white, which repeated in this manner and contained around 195 drawings. One of Lorrain's biographers. reported that the purpose in creating the Liber Veritatis was to protect Lorrain against forgery (it is not clear 'how far the objective of protection against forgery can be accepted as an adequate example of the book's raison d'être') In fact. any comparison between drawings and paintings goes to show that the former were designed to serve as a 'check' on the latter and from the Liber any very careful observer could tell whether a given painting was a forgery or not. Similar techniques are being used today. ImageLock, for instance, keeps a central database of image digests and periodically searches the Web for images having the same digest. Tracking systems based on private watermarks also require central databases. Unfortunately, apart from the extent of the problem (which is now global) nothing much has changed, since such services still do not provide any proof of infringement.

© 2000-2002 by WatermarkingWorld Design and Concept by Martin Kutter

Nelson, Robert P.

From: Kieper, Cynthia L.

Sent: Tuesday, October 28, 2003 10:49 AM

To: Nelson, Robert P.

Subject: Assembly bill 584; Representative Schneider

Dear sir,

Representative Schneider would like a (sub-amendment?) I believe it's called on AB 584. He asking that digital photography technology or audio recordings must have technology that cannot be altered. He wants it defined within the rules of evidence. In addition he wants the penalty to be a class A misdemeanor along with the perjury charges. If it involves the DA, Assistant DA or private attorney, grounds for disbarment.

Cynthia 266-0215



State of Misconsin 2003 - 2004 LEGISLATURE

LRBs0241/P1

P-N

RPNJd

PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION

ASSEMBLY SUBSTITUTE AMENDMENT,

TO 2003 ASSEMBLY BILL 584

	AN ACT; relating to: admissibility of digitally produced photograph, fill audio,
2	or video.
3	The people of the state of Wisconsin, represented in senate and assembly, do enact as follows: National (1) of the statutes is renumbered 910.01 (12) Section 2. 910.01 (1g) of the statutes is created to read:
5 6	910.01 (1g) DIGITAL REPRESENTATION. "Digital representation" means any recording or image of a person, place, document, sound, or event that is created or
7 (8)com	stored by data in the form of numerical digits. renumbered 910.01 (4m) and forent Section 3. 910.01 (2) of the statutes is amended to read:
9	910.01 (2) PHOTOGRAPHS. "Photographs" include still photographs, X-ray films, and motion pictures, and digital representations.
11	SECTION 4. 910.025 of the statutes is created to read:

0

910.025 Inadmissibility of a digital representation. In any action or	
proceeding, except an action under s. 948.05 or 948.12, a digital representation in the	
form of a photograph, film, motion picture, audio, or video is not admissible for	
purposes of proving the content of that digital representation unless that digital	
representation is in a format that includes information that cannot be identified or	
manipulated and that shows that the digital representation has not been altered	
from its original representation. — [precedes 946.31]	
SECTION 5. Subchapter III (title) of chapter 946 of the statutes have statutes and the statutes and the statutes are statutes are statutes and the statutes are statutes ar	9
MANN'is amended to read: CHAPTER 946 COARS SUBCHAPTER III CNO CO	
PERJURY, DIGITAL ALTERATION, AND FALSE SWEARING	
×	
SECTION 6. 946.33 of the statutes is created to read:	
946.33 Alteration of a digital representation. (1) In this section, "digital	
representation" means any recording or image of a person, place, document, sound,	
or event that is created or stored by data in the form of numerical digits.	
(2) Whoever admits into evidence a digital representation for the purpose of	
proving the content of that digital representation knowing that the digital	
representation has been altered from its original representation is guilty of a class	
A misdemeanor.	
Section 7. Initial applicability.	
(1) This act first applies to actions commenced on the effective date of this	
subsection.	
(ENTD.)	

d-note

SECTION # AM; 802.05 (1)(c)

document and the signing party or his or her attorney retains the original document.

802.05(1) (2m)
(c) The requirement of a handwritten signature subscribing pleadings, motions or other papers filed in court may be satisfied by a duplicate, as defined in s. 910.01 (4), if a handwritten signature appears on the original

(end ins 1-3)

DRAFTER'S NOTE FROM THE LEGISLATIVE REFERENCE BUREAU

LRBs0241/P1dn

The Supreme Court disciplines members of the State Bar of Wisconsin, and the legislature has no authority to regulate or discipline those members. I therefore did not add language regarding the disbarment of DAs, etc., if they use altered digital representations. Section 946.31 of the statutes already covers perjury, so no change is needed in that statute.



I made this a preliminary draft because I was unsure if I did what you intended.

Robert P. Nelson Senior Legislative Attorney Phone: (608) 267–7511

E-mail: robert.nelson@legis.state.wi.us

DRAFTER'S NOTE FROM THE LEGISLATIVE REFERENCE BUREAU

LRBs0241/P1dn RPN:jld:jf

November 4, 2003

The Supreme Court disciplines members of the State Bar of Wisconsin, and the legislature has no authority to regulate or discipline those members. I therefore did not add language regarding the disbarment of DAs, etc., if they use altered digital representations. Section 946.31 of the statutes already covers perjury, so no change is needed in that statute.

I made this a preliminary draft because I was unsure if I did what you intended.

Robert P. Nelson Senior Legislative Attorney

Phone: (608) 267–7511

 $E-mail:\ robert.nelson@legis.state.wi.us$

Nelson, Robert P.

From: Emery, Lynn

Sent: Tuesday, November 04, 2003 9:32 AM

To: Nelson, Robert P.

Subject: FW: Draft review: LRB 03s0241/P1 Topic: Use of digital technology in evidence only if cannot be

altered

-----Original Message-----From: Schneider, Marlin

Sent: Tuesday, November 04, 2003 9:32 AM

To: Emery, Lynn

Subject: RE: Draft review: LRB 03s0241/P1 Topic: Use of digital technology in evidence only if cannot be

altered

This looks fine me. - Marlin

-----Original Message-----From: Emery, Lynn

Sent: Tuesday, November 04, 2003 9:25 AM

To: Rep.Schneider

Subject: Draft review: LRB 03s0241/P1 Topic: Use of digital technology in evidence only if

cannot be altered

Following is the PDF version of draft LRB 03s0241/P1 and drafter's note.



1

2

3

4

5

6

7

8

9

10

11

State of Misconsin 2003 – 2004 LEGISLATURE

LRBs0241/PK RPN:jld:jf

PREMINARY DRAFT - NOT READY FOR INPRODUCTION ASSEMBLY SUBSTITUTE AMENDMENT, TO 2003 ASSEMBLY BILL 584

AN ACT to renumber 910.0

AN ACT to renumber 910.01 (1) and 910.01 (4); to renumber and amend 910.01 (2); to amend 802.05 (1) (c) and subchapter III, (title) of chapter 946 [precedes 946.31]; and to create 910.01 (1g), 910.025 and 946.33 of the statutes; relating to: admissibility of digitally produced photograph, film, motion picture, audio, or video.

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

Section 1. 802.05 (1) (c) of the statutes is amended to read:

802.05 (1) (c) The requirement of a handwritten signature subscribing pleadings, motions or other papers filed in court may be satisfied by a duplicate, as defined in s. 910.01 (4) (2m), if a handwritten signature appears on the original document and the signing party or his or her attorney retains the original document.

SECTION 2. 910.01 (1) of the statutes is renumbered 910.01 (5m).

1	SECTION 3. 910.01 (1g) of the statutes is created to read:
2	910.01 (1g) DIGITAL REPRESENTATION. "Digital representation" means any
3	recording or image of a person, place, document, sound, or event that is created or
4	stored by data in the form of numerical digits.
5	SECTION 4. 910.01 (2) of the statutes is renumbered 910.01 (4m) and amended
6	to read:
7	910.01 (4m) PHOTOGRAPHS. "Photographs" include still photographs, X-ray
8	films, and motion pictures, and digital representations.
9	SECTION 5. 910.01 (4) of the statutes is renumbered 910.01 (2m).
10	SECTION 6. 910.025 of the statutes is created to read:
11	910.025 Inadmissibility of a digital representation. In any action or
12	proceeding, except an action under s. 948.05 or 948.12, a digital representation in the
13	form of a photograph, film, motion picture, audio, or video is not admissible for
14	purposes of proving the content of that digital representation unless that digital
15	representation is in a format that includes information that cannot be identified or
16	manipulated and that shows that the digital representation has not been altered
17	from its original representation.
18	SECTION 7. Subchapter III, (title) of chapter 946 [precedes 946.31] of the
19	statutes is amended to read:
20	CHAPTER 946
21	SUBCHAPTER III
22	PERJURY, DIGITAL ALTERATION,
23	AND FALSE SWEARING
24	SECTION 8. 946.33 of the statutes is created to read:

946.33 Alteration of a digital representation. (1) In this section, "digital
representation" means any recording or image of a person, place, document, sound,
or event that is created or stored by data in the form of numerical digits.
(2) Whoever admits into evidence a digital representation for the purpose of
proving the content of that digital representation knowing that the digital
representation has been altered from its original representation is guilty of a Class
A misdemeanor.
Section 9. Initial applicability.
(1) This act first applies to actions commenced on the effective date of this
subsection.

(END)